I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being transmitted today via the Office electronic filing system in accordance with 37 CFR §1.6 (a)(4).

Date: September 24, 2010 Signature: _____
Sanro Zlobec, Reg. No. 52,535

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re:	U.S. Patent Application of Tet Hin YEAP *et al.*		
App. No.:	10/673,509	Group Art Unit:	2455
Filed:	September 30, 2003	Examiner:	Shawki Saif ISMAIL
For:	SYSTEM AND METHOD FOR SECURE ACCESS		

APPEAL BRIEF UNDER 37 CFR §41.37

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Further to the Notice of Appeal filed June 22, 2010 and the Notice of Panel Decision on Pre-Appeal Brief Review mailed August 31, 2010, submitted herewith is an Appeal Brief in accordance with 37 CFR §41.37. The fee for filing a brief in support of an appeal as set forth in 37 CFR §41.20(b)(2) is also being submitted herewith.

If any further fees are due, the Director is hereby authorized to debit the required amount from deposit account no. 19-2550 and is respectfully requested to advise the Applicant accordingly.

I. 37 CFR §41.37 (c)(1)(i) - Real Party in interest

The real party in interest is the assignee of the entire interest in the present patent application, namely BCE, Inc.

II. 37 CFR §41.37 (c)(1)(ii) - Related Appeals and Interferences

Applicants believe that there are no related appeals or interferences.

III. 37 CFR §41.37 (c)(1)(iii) - Status of the Claims

Claims 35-41, 44-45, 47-50, 52, 54-55, 67-69 and 83 are rejected.

Claims 1-34, 42-43, 46, 51, 53 and 74-82 are cancelled.

Claims 56-66 and 70-73 are withdrawn.

Claims 35-41, 44-45, 47-50, 52, 54-55, 67-69 and 83 are being appealed.

IV. 37 CFR §41.37 (c)(1)(iv) - Status of Amendments

The last amendments to the claims were made in the Applicant's communication to the Patent Office dated May 14, 2009, which was responsive to the Non-Final Office Action mailed February 3, 2009.

No Final Office Action has been mailed since then (although a further Non-Final Office Action was mailed on February 22, 2010, in response to which no amendments were made).

V. 37 CFR §41.37 (c)(1)(v) - Summary of Claimed Subject Matter

In the following, any association between claim language and the specification/drawings serves merely as a guide to facilitate understanding and is not to be considered limiting.

Claim 35

Claim 35 is directed to an authentication system.	(Fig 1, 30; page 4, lines 17-22)
The authentication system comprises an access controller	(Fig 1, 54; page 5, lines 1-11)
that is operable to communicate with a client	(Fig 1, 42; page 5, lines 21-28)
via a first communication medium.	(page 5, lines 1-11; page 19, line 1 –page 20, line 3)
The authentication system further comprises an authentication server	(Fig 1, 38; page 5, lines 12-17)
that is operable to communicate with the client and the access controller via a second communication medium.	(page 5, lines 12-20; page 19, line 1 –page 20, line 3)
The authentication server is further operable to deliver a first key to the client	(Fig. 3, 355; page 5, lines 17-26; page 15, lines 1-8)
and a second key to the access controller.	(Fig 2, 240; page 5, lines 17-26; page 9, lines 19-21)
The second key is complementary to the first key	(page 5, lines 15-19)
such that when the client and the access controller are connected, communications therebetween can be encrypted using the keys.	(page 5, lines 13-20, page 5, lines 21-28; Fig 4, 420-430; page 16, lines 12-21; page 18, lines 7-16)
The access controller is further operable to selectively pass instructions received from the client to a computer attached to the access controller if a verification protocol utilizing the keys is met	(Fig 4, 435-440; page 16, line 22 – page 17, line 3).
The first key is delivered to the client only after the second key has been successfully delivered to the access controller.	(Claims 7 and 17 as originally filed)

Claim 45

Claim 45 is directed to an access controller	(Fig 1, 54; page 5, lines 5-9; page 6, lines 1-7)
for intermediating communications between	(page 6, lines 1-7)
an interface	(Fig 1, 58; page 5, lines 6-9)
and a computer	(Fig. 1, 34, 50; page 5, lines 1-11; page 19, lines 1-4; page 20, lines 4-9)
and operable to store a second key complementary to a first key.	(Table 1; Fig 1, 62; page 5, lines 15-26; page 6, line 12 – page7, line 17; page 9, lines 19-21; Table III; page 11, lines 1-3; page 15, lines 1-8)
The access controller is further operable to communicate with a client via the interface.	(Fig 1, 58; page 5, lines 1-11)
The client is operable to store the first key	(Table V; Fig 1, 70; page 5, lines 21-28; page 12, line 18 – page 13, line 2; Table VII)
and to receive instructions from a user.	(page 16, lines 8-11)
The access controller is still further operable to selectively pass the instructions to the computer if a verification protocol utilizing the keys is met.	(Fig 4, 435-440; page 16, line 22 – page 17, line 3)
The verification protocol includes the generation of a random number by the client and an encryption of the random number by the client using the first key.	(Fig. 4, 415-420; page 16, lines 12-18)
The random number and the encrypted random number are delivered from the client to the access controller.	(Fig. 4, 425; page 16, lines 12-18)
The encrypted random number is decrypted using the second key by the access controller	(Fig. 4, 430; page 16, lines 19-21)
and a comparison of the random number and the decrypted number is made.	(Fig. 4, 435; page 16, lines 22-27)
If the comparison finds a match of the random number with the decrypted random number, the decision is made to pass at least a portion of the instructions.	(Fig. 4, 435-440; page 16, line 22 – page 17, line 3)
If no match is found, a decision is made not to pass the at least a portion of the instructions.	(Fig. 4, 435; page 16, lines 22-27)
The first key is obtained by the client only after the	(Claims 7 and 17 as originally filed)

second key has been successfully obtained by the access controller	

Claim 67

Claim 67 is directed to a method	(Fig. 4, 400; page 15, line 17 – page 17, line 5)
of securing access between a client	(Fig. 1, 42; page 5, lines 21-28)
and a computer	(Fig. 1, 34, 50; page 5, lines 1-11; page 19, lines 1-4; page 20, lines 4-9)
having an access controller	(Fig 1, 54; page 5, lines 1-11)
intermediate the client and the computer. The client receives an instruction destined for the computer	(Fig. 4, 410; page 16, lines 8-11)
and generates a random number.	(Fig. 4, 415, page 16, lines 12-18)
The client encrypts the random number using a first key.	(Fig.4, 420; page 5, lines 17-26; page 16, lines 12-18)
The random number, the encrypted random number and the instruction are delivered to the access controller.	(Fig. 4, 425; page 16, lines 12-18)
The access controller decrypts the encrypted random number using a second key, the second key being complementary to the first key.	(Fig. 4, 430; page 5, lines 17-26; page 16, lines 19-21)
The random number and the decrypted number are compared.	(Fig. 4, 435; page 16, lines 22-27)
If the comparison finds a match of the random number with the decrypted number, at least a portion of the instruction is passed to the computer.	(Fig. 4, 440; page 16, line 22 – page 17, line 3)
If no match is found, the at least a portion is discarded.	(Fig. 4, path "Discard Instruction"; page 16, lines 22-27)

Claim 68

Claim 68 is directed to an authentication server	(Fig 1, 38; page 5, lines 12-17)
comprising an interface	(page 5, lines 13-20)
for communicating with a client	(Fig. 1, 42; page 5, lines 21-28)
and an access controller	(Fig. 1, 54; page 5, lines 1-11)

via a communication medium	(Fig 1, 46; page 5, lines 1-11; page 19, line 1- page 20, line 3)
and a processing unit.	(page 5, lines 13-20)
The processing unit is operable to determine a first key for delivery to the client and a second key for delivery to the access controller.	(page 5, lines 13-26; page 9, lines 15-18)
The first key is delivered to said client only after the second key has been successfully delivered to the access controller.	(Claims 7 and 17 as originally filed)
When the access controller and the client are connected, the access controller selectively passes instructions from the access controller if a verification protocol utilizing the keys is met.	(page 6, lines 1-7; Fig. 4, 435-440; page 16, line 22 – page 17, line 3)

VI. 37 CFR §41.37 (c)(1)(vi) - Grounds of rejection to be reviewed on Appeal

(a) Whether claims 35-39, 41, 44 and 68-69 are unpatentable under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 7,395,549 to Perlman et al. (hereinafter "Perlman");

(b) Whether claims 40, 45, 47-50, 52, 54-55, 67 and 83 are unpatentable under 35 U.S.C. §103(a) as being obvious over Perlman in view of "Official Notice".

VII. 37 CFR §41.37 (c)(1)(vii) - Arguments

(a) REJECTION OF CLAIMS 35-39, 41, 44 AND 68-69 UNDER 35 U.S.C. §102(E) AS BEING ANTICIPATED BY PERLMAN

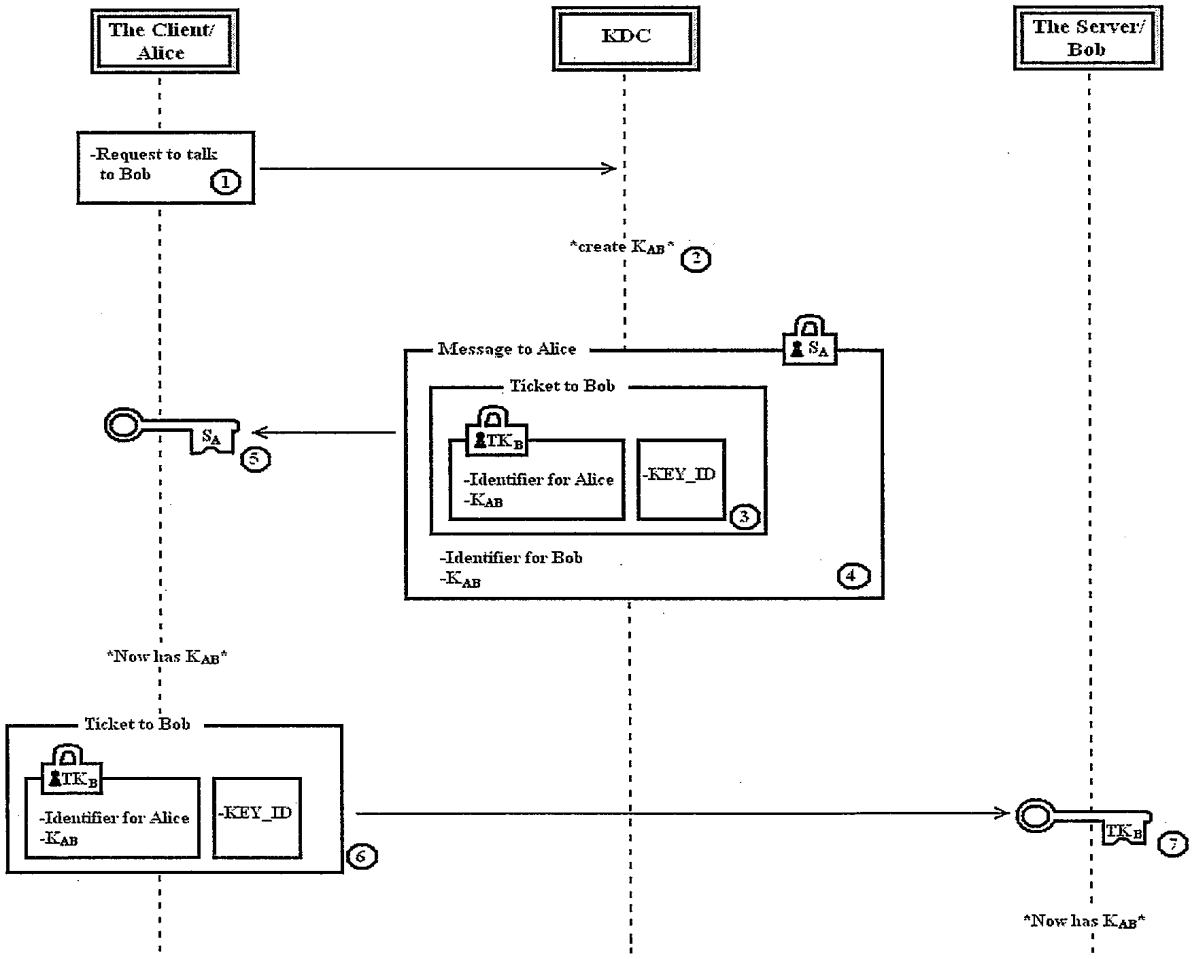
I. The Cited Art Lacks At Least One Element Required to Establish Anticipation

Quoting from *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987), the current edition of the MPEP states: "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference."

It is respectfully submitted that Perlman, the single prior art reference cited in the Office Action mailed February 22, 2010, lacks at least one element required to establish anticipation of claims 35 and 68.

Specifically, Perlman relates to providing a key distribution center while avoiding storing long-term server secrets. In particular, a client (Alice) and a server (Bob) make use of a key distribution center (KDC) to permit communication between each other. To communicate with Bob, Alice sends a request to the KDC. The KDC then "creates a session key, K_{AB}, to be used in communications between Alice and Bob. KDC 102 retrieves Bob's temporary secret key, TK_B, and then creates a "ticket to Bob" by using TK_B to encrypt the identifier for "Alice" and K_{AB}, and by attaching the key identifier for TK_B, KEY_ID, in the clear" (col. 6, lines 56-61).

Perlman's method of establishing communication between Alice and Bob is now described with reference to the Figure included herewith:


The Client/ Alice
KDC
The Server/ Bob
-Request to talk to Bob
1
create K_{AB}
2
Message to Alice
S_A
Ticket to Bob
TK_B
-Identifier for Alice
-K_{AB}
-KEY_ID
3
-Identifier for Bob
-K_{AB}
4
S_A
5
Now has K_{AB}
Ticket to Bob
TK_B
-Identifier for Alice
-K_{AB}
-KEY_ID
6
TK_B
7
Now has K_{AB}

As shown, communication is initiated by the client/Alice by sending the KDC a request ①, to talk to the server/Bob (col. 6, ln. 56-61). Upon receiving this request, at ②, the KDC creates K_{AB}, an encryption key that is to be used for communication between Alice and Bob (col. 6, ln. 56-58). The KDC then generates a ticket to Bob ③, which comprises an Identifier for Alice and K_{AB}, both encrypted with TK_B, and a KEY_ID indicative of TK_B (col. 6, ln. 58-61). The KDC then generates a Message to Alice ④, which comprises the ticket to Bob as well as an Identifier for Bob and (unencrypted) K_{AB} (col. 6, ln. 62-65). The Message to Alice is encrypted using S_A, which is a function of Alice's password and sent to Alice. Upon reception of the Message to Alice, the client/Alice decrypts ⑤, the Message to Alice using S_A and derives the Identifier for Bob, K_{AB} and the Ticket to Bob (col. 6, ln. 66-67). The client/Alice now has K_{AB}. Alice then sends ⑥, the Ticket to Bob to the server/Bob (col. 7, ln. 5-6) who decrypts ⑦ the Ticket to Bob using TK_B (col. 7, ln. 8-9). Bob now also has K_{AB}. Alice can now prove it also knows K_{AB} and encrypted communication can take place between Bob and Alice.

Thus, one can make the following observations regarding Perlman:

i. The session key, K_{AB}, is necessarily delivered to the client/Alice before it can be delivered to the server/Bob, since the client/Alice is responsible for delivering it (within the Ticket to Bob) to the server/Bob.

ii. No authentication server ever sends an encryption key for communication between Alice and Bob to the server/Bob. Rather, the KDC sends two copies of K_{AB} to the client/Alice (one of which is within the Ticket to Bob) and the client/Alice is responsible for transmitting the K_{AB} (within the Ticket to Bob) to the server/Bob. In fact no one entity sends two keys (or even one same key) to two different recipients.

iii. The same session key K_{AB} is used by both the client/Alice and the server/Bob for communication therebetween. There are no complementary keys.

iv. No two entities communicate together using two complementary keys. Alice and Bob, communicate using K_{AB} alone.

Perlman therefore can not be held to teach delivery from an authentication server of a first key to a client and a second key to an access controller. Perlman's failure to teach such a delivery also implies a failure by Perlman to provide the second key complementary to the first key. And, naturally, Perlman's outright failure to deliver from an authentication server a first key to a client and a second key to an access controller implies that it is impossible for the first key to be delivered to the client only after the second key has been successfully delivered to the access controller.

The Applicant would also like to address an apparent misinterpretation of Perlman by the Examiner. In alleging that "said access controller [...] operable to deliver a first key to said client and a second key to said controller" is disclosed by Perlman, the Examiner cites not only sections of Perlman describing dissemination of K_{AB} but also a section of Perlman that describes the establishment of a temporary secret key TK_B for the server/Bob. It thus appears that the Examiner interprets TK_B and K_{AB} as a set of a first and second key delivered respectively to a client and an access controller by an authentication server, and complementary to one another, and used for communications between a client and an access controller when they are connected. However, it will be appreciated that:

i. TK_B and K_{AB} are not delivered by the same entity (authentication server or otherwise – K_{AB} is delivered by the KDC to the client/Alice, while the TK_B is created by the server/Bob and delivered to the KDC);

ii. TK_B is not complementary to K_{AB}; and

iii. TK_B is not used to encrypt communication from Alice to Bob or *vice versa*. Thus it would be incorrect to interpret TK_B and K_{AB} as the first and second keys recited in claim 35.

Thus, it can be appreciated that Perlman completely fails to disclose:

- "an authentication server operable to communicate with said client and said access controller via a second communication medium and further **operable to deliver a first key to said client and a second key to said access controller, said second key being complementary to said first key** such that when said client and said access controller are connected, communications therebetween can be encrypted using said keys";
- "wherein said access controller is operable to selectively pass instructions received from said client to a computer attached to said access controller if a verification protocol utilizing said keys is met";
- "said first key is delivered to said client only after said second key has been successfully delivered to said access controller".

It is therefore respectfully submitted that Perlman lacks at least one element required to establish anticipation of claim 35.

Claim 68 includes features similar to those of claim 35 and therefore the same arguments apply to claim 68.

II. The Rejection is Defective Because it Fails to Identify New Grounds of Rejection

In the Applicant's May 14, 2009 response to the Office Action of February 3, 2009, claim 35 had been amended in order to introduce therein the subject matter of former dependent claim 42 which was cancelled. A similar amendment was made to claim 68 and remarks were made to address the Examiner's rejection of claims 35 and 68, which addressed and rebutted the Examiner's position with respect to former dependent claim 42.

In the subsequent Office Action dated February 22, 2010, the Examiner states on page 2 that "Applicants (*sic*) arguments have been fully considered and are persuasive, however upon further review and consideration a new grounds of rejection is hereby made" (emphasis added). The Examiner also states on page 5 of the Office Action that "Applicants' arguments have been fully considered however they are deemed moot in view of the new ground(s) of rejection" (emphasis added).

Yet, in the rejection of claims 35 and 68, the Examiner provides no such "new grounds of rejection". Rather, regarding claim 35, the Examiner repeats portions of the arguments made in an earlier Office Action in respect of former claim 35, and merely cites a passage of Perlman which, it is remarked, was already previously cited against former claim 42 and dealt with in the previous response. Regarding claim 68, the Examiner merely states that this claim "[does] not teach or define any new limitations beyond the claims above, therefore, [it] is rejected for similar reasons."

Since no "new grounds of rejection" have in fact been identified, and since the Examiner considers that the previously submitted arguments were in fact

"persuasive", the only possible conclusion is that claims 35 and 68 are in fact not meant to be rejected.

III. Conclusion

In view of the arguments presented above in **(a) I** and **(a) II**, the Examiner is therefore respectfully requested to withdraw the rejection of claims 35 and 68 under §102(e).

Also, each of claims 36-39, 41, 44 and 69 is dependent on one of claims 35 and 68, and therefore benefit from the same arguments as those made in support of claims 35 and 68. Withdrawal of the rejection of claims 36-39, 41, 44 and 69 under §102(e) is therefore respectfully requested.

(b) REJECTION OF CLAIMS 40, 45, 47-50, 52, 54-55, 67 AND 83 UNDER 35 U.S.C. §103(A) AS BEING OBVIOUS OVER PERLMAN IN VIEW OF "OFFICIAL NOTICE"

Claims 45, 47-50, 52, 54-55 and 67

I. The Examiner Has Not Made a Proper Determination of Obviousness

It is respectfully submitted that in the Office Action mailed February 22, 2010, the Examiner did not fully examine the subject matter of the claims. In fact, the Examiner appears to have completely failed to address any of the following features recited in claim 45 (and similar features in claim 67):

> "a generation of a random number by said client,
> an encryption of said random number by said client using said first key,

a delivery of said random number and said encrypted random number from said client to said access controller,
a decryption of said encrypted random number using said second key by said access controller,
a comparison of said random number and said decrypted number,
and a decision to pass at least a portion of said instructions if said comparison finds a match of said random number with said decrypted number,
and a decision not to pass said at least a portion of said instructions if no match is found."

Specifically, although the Examiner admits that Perlman fails to teach the above features, he merely states (see page 5 of the Office Action) that "it would be obvious [...] to incorporate the teachings of Official Notice into the system or Perlman in order to allow the server to verify the client's integrity".

Given that nowhere does the alleged "Official Notice" relate to random numbers or any of the above features of claims 45 and 67, it should be readily apparent that the Examiner has not established that claims 45 and 67 are obvious, and in fact it is respectfully submitted that the rejection is defective for having failed to identify the presence of numerous claimed elements in the cited art.

Notwithstanding the above, even if a hypothetical reference did teach – as the Examiner alleges – "the use of three way handshaking protocol in a PKI system to verify the client's integrity", the combination of such a hypothetical reference and Perlman would still not teach anything related to the generation of a random number. This is quite simply because three way handshaking does not in any way imply random number generation. Since Perlman also does not pertain to random

number generation[1], it therefore follows that the combination Perlman and a hypothetical "three way handshaking" reference would still not teach anything related to:

i. encrypting a random number using a first key;
ii. delivering a random number from a client to an access controller;
iii. delivering an encrypted random number from the client to the access controller;
iv. decrypting the encrypted random number by the access controller using a second key (there is also no "first" and "second" complementary keys in Perlman, as discussed above);
v. comparing the random number and the decrypted version of the encrypted random number; or
vi. a decision to pass at least a portion of an instruction (received from the client) if the comparison finds a match.

Therefore, Applicant respectfully submits that the differences between the subject matter of claims 45 (and 67) and the cited art are indubitably beyond the level of ordinary skill in the art. As such, it is respectfully submitted that the Examiner has not made a proper determination of obviousness under 35 USC §103.

II. The Rejection of Claims 45 and 67 is Defective Due to Improper Official Notice

In addition to the above, it is respectfully submitted that the Examiner's rejection in the Office Action mailed February 22, 2010 is defective due to improper Official Notice. In particular, the Examiner states "Official Notice teaches the use of three way handshaking protocol in a PKI system to verify the client's

[1] whether in the creation of the session key K_{AB} (which is created by the KDC and sent to Alice), the temporary secret key TK_B (which is created by the server/Bob and sent to the KDC) or S_A (which is a function of Alice's password).

integrity". However, and with all due respect, Applicant believes that it is improper to suggest that Official Notice "teaches" something. Rather, if Official Notice is taken, it should be taken of a fact that is considered to be well known or part of the common general knowledge in the art, and capable of such instant and unquestionable demonstration as to defy dispute (*In Re Ahlert* 165 USPQ 418). It follows that Official Notice should not "teach" anything.

Furthermore, no explicit basis has been set forth in support of the Official Notice taken by the Examiner, and it is respectfully submitted that, in the absence of such an explicitly set forth basis, it is inappropriate (see MPEP 2144.03) for the Examiner to take Official Notice that "the use of three way handshaking protocol in a PKI system to verify the client's integrity" is known. Moreover, it is respectfully submitted that any assertion of technical facts should be supported by references (*ibid*), of which the Examiner provides none.

For the above reasons, it is respectfully submitted that the Official Notice taken by the Examiner does not appropriately constitute part of the scope and content of the prior art that can be relied upon by the Examiner in formulating an obviousness rejection.

III. Conclusion

In view of the arguments presented above, the Examiner is respectfully requested to withdraw the rejection of claims 45 and 67 under §103(a).

Also, each of claims 47-50, 52 and 54-55 is dependent on claim 45, and therefore benefits from the same argument as that which applies to claim 45. Withdrawal of the rejection under §103(a) of claims 47-50, 52 and 54-55 is therefore respectfully requested.

Claim 83

Claim 83 is dependent on claim 35, and therefore includes the features of claim 35 already shown to be absent from Perlman. Specifically, it has been shown earlier in this Appeal Brief that Perlman fails to disclose:

- "an authentication server operable to communicate with said client and said access controller via a second communication medium and further operable to deliver a first key to said client and a second key to said access controller, said second key being complementary to said first key such that when said client and said access controller are connected, communications therebetween can be encrypted using said keys";
- "wherein said access controller is operable to selectively pass instructions received from said client to a computer attached to said access controller if a verification protocol utilizing said keys is met";
- "said first key is delivered to said client only after said second key has been successfully delivered to said access controller".

It should thus be clear that significant differences exist between the claimed invention and Perlman, and that these differences are beyond the level of ordinary skill in the art.

Next, the Examiner states (see page 5 of the Office Action) that "Official Notice teaches the use of three way handshaking protocol in a PKI system to verify the client's integrity" and that that "it would be obvious [...] to incorporate the teachings of Official Notice into the system or Perlman in order to allow the server to verify the client's integrity".

Aside from the fact that the Official Notice taken by the Examiner does not appropriately constitute part of the scope and content of the prior art that can be

relied upon by the Examiner in formulating an obviousness rejection[2], it is respectfully submitted that the alleged "Official Notice" – even if it did teach "the use of three way handshaking protocol in a PKI system to verify the client's integrity" – would still not teach or suggest any of the above-mentioned features of claim 40, namely:

- "an authentication server operable to communicate with said client and said access controller via a second communication medium and further operable to deliver a first key to said client and a second key to said access controller, said second key being complementary to said first key such that when said client and said access controller are connected, communications therebetween can be encrypted using said keys";
- "wherein said access controller is operable to selectively pass instructions received from said client to a computer attached to said access controller if a verification protocol utilizing said keys is met";
- "said first key is delivered to said client only after said second key has been successfully delivered to said access controller".

Stated differently, it should be clear that the Official Notice – notwithstanding its impropriety – does nothing to remedy the deficiencies of Perlman. Therefore, Applicant respectfully submits that the differences between the claimed invention and the cited art remain indubitably beyond the level of ordinary skill in the art. As such, it is respectfully submitted that the Examiner has not made a proper determination of obviousness under 35 USC §103 and it is respectfully requested that the rejection of claim 83 under 35 USC §103 be withdrawn.

[2] Specifically, the Official Notice does not recite a fact that is considered to be well known or part of the common general knowledge in the art, and capable of such instant and unquestionable demonstration as to defy dispute (*In Re Ahlert* 165 USPQ 418). Nor does the Examiner provide any explicit basis been set forth in support of the Official Notice. Moreover, the Examiner provides no references in support of any assertion of technical facts.

Claim 40

Claim 40 is dependent on claim 35, and therefore includes the features of claim 35 already shown to be absent from Perlman. Specifically, it has been shown earlier in this Appeal Brief that Perlman fails to disclose

- "an authentication server operable to communicate with said client and said access controller via a second communication medium and further operable to deliver a first key to said client and a second key to said access controller, said second key being complementary to said first key such that when said client and said access controller are connected, communications therebetween can be encrypted using said keys";
- "wherein said access controller is operable to selectively pass instructions received from said client to a computer attached to said access controller if a verification protocol utilizing said keys is met";
- "said first key is delivered to said client only after said second key has been successfully delivered to said access controller".

It should thus be clear that significant differences exist between the claimed invention and Perlman, and that these differences are beyond the level of ordinary skill in the art.

In addition, claim 40 includes the additional feature of:

- "wherein said verification protocol includes a generation of a random number by said client, an encryption of said random number by said client using said first key, a delivery of said random number and said encrypted random number from said client to said access controller, a decryption of said encrypted random number using said second key by said access controller, a comparison of said random number and said decrypted number, and a decision to pass at least a portion of said instructions if said

comparison finds a match of said random number with said decrypted number, and a decision not to pass said at least a portion of said instructions if no match is found".

Now, the Examiner concedes that this additional feature is not taught in Perlman. Applicant therefore respectfully submits that even ***greater*** differences exist between the claimed invention and Perlman, and that these differences are beyond the level of ordinary skill in the art.

Next, the Examiner states (see page 5 of the Office Action) that "Official Notice teaches the use of three way handshaking protocol in a PKI system to verify the client's integrity" and that that "it would be obvious [...] to incorporate the teachings of Official Notice into the system or Perlman in order to allow the server to verify the client's integrity".

Aside from the fact that the Official Notice taken by the Examiner does not appropriately constitute part of the scope and content of the prior art that can be relied upon by the Examiner in formulating an obviousness rejection[3], it is respectfully submitted that the alleged "Official Notice" – even if it did teach "the use of three way handshaking protocol in a PKI system to verify the client's integrity" – would not teach or suggest any of the above-mentioned features of claim 40, namely:

- "an authentication server operable to communicate with said client and said access controller via a second communication medium and further operable to deliver a first key to said client and a second key to said access controller, said second key being complementary to said first key such that when said client and said access controller are connected, communications therebetween can be encrypted using said keys";

[3] ibid

- "wherein said access controller is operable to selectively pass instructions received from said client to a computer attached to said access controller if a verification protocol utilizing said keys is met";
- "said first key is delivered to said client only after said second key has been successfully delivered to said access controller";
- "wherein said verification protocol includes a generation of a random number by said client, an encryption of said random number by said client using said first key, a delivery of said random number and said encrypted random number from said client to said access controller, a decryption of said encrypted random number using said second key by said access controller, a comparison of said random number and said decrypted number, and a decision to pass at least a portion of said instructions if said comparison finds a match of said random number with said decrypted number, and a decision not to pass said at least a portion of said instructions if no match is found".

Stated differently, it should be clear that the Official Notice – notwithstanding its impropriety – does nothing to remedy the deficiencies of Perlman. Therefore, Applicant respectfully submits that the differences between the claimed invention and the cited art remain indubitably beyond the level of ordinary skill in the art. As such, it is respectfully submitted that the Examiner has not made a proper determination of obviousness under 35 USC §103 and it is respectfully requested that the rejection of claim 40 under 35 USC §103 be withdrawn.

VIII. 37 CFR §41.37 (c)(1)(viii) - Claim Appendix

The following is a listing of the claims involved in the present appeal.

1. – 34. (*cancelled*)

35. An authentication system, comprising:

an access controller operable to communicate with a client via a first communication medium; and

an authentication server operable to communicate with said client and said access controller via a second communication medium and further operable to deliver a first key to said client and a second key to said access controller, said second key being complementary to said first key such that when said client and said access controller are connected, communications therebetween can be encrypted using said keys; and wherein said access controller is operable to selectively pass instructions received from said client to a computer attached to said access controller if a verification protocol utilizing said keys is met;

wherein said first key is delivered to said client only after said second key has been successfully delivered to said access controller.

36. The authentication system according to claim 35, wherein said authentication server is operable to generate said first key and said second key.

37. The authentication system according to claim 35, wherein said first key is a public encryption key and said second key is a private encryption key complementary to said public encryption key.

38. The authentication system according to claim 35, wherein each of said first communication medium and said second communication medium is selected from the group of networks consisting of the Internet, the PSTN, a local area network, and a wireless network.

39. The authentication system according to claim 35, wherein said computer is a telecommunications switch.

40. The authentication system according to claim 35, wherein said verification protocol includes a generation of a random number by said client, an encryption of said random number by said client using said first key, a delivery of said random number and said encrypted random number from said client to said access controller, a decryption of said encrypted random number using said second key by said access controller, a comparison of said random number and said decrypted number, and a decision to pass at least a portion of said instructions if said comparison finds a match of said random number with said decrypted number,

and a decision not to pass said at least a portion of said instructions if no match is found.

41. The authentication system according to claim 35, wherein said instructions are encrypted by said client using said first key and said verification protocol is based on a successful decryption of said instructions by said access controller using said second key.

42. (*cancelled*)

43. (*cancelled*)

44. The authentication system according to claim 35, wherein said access controller contains a preset second key and said authentication server maintains a record of said preset second key; said authentication server operable to deliver said first key and said second key only if said access controller successfully transmits said preset second key to said authentication server and said transmitted preset second key matches said authentication server's record thereof.

45. An access controller for intermediating communications between an interface and a computer and operable to store a second key complementary to a first key; said

access controller operable to communicate with a client via said interface; said client operable to store said first key and to receive instructions from a user; said access controller operable to selectively pass said instructions to said computer if a verification protocol utilizing said keys is met;

wherein said verification protocol includes a generation of a random number by said client, an encryption of said random number by said client using said first key, a delivery of said random number and said encrypted random number from said client to said access controller, a decryption of said encrypted random number using said second key by said access controller, a comparison of said random number and said decrypted number, and a decision to pass at least a portion of said instructions if said comparison finds a match of said random number with said decrypted number, and a decision not to pass said at least a portion of said instructions if no match is found; wherein said access controller is operable to obtain said second key from an authentication server and said client is operable to obtain said first key from said authentication server; wherein said first key is obtained by said client only after said second key has been successfully obtained by said access controller.

46. (*cancelled*)

47. The access controller of claim 45, wherein said authentication server is operable to generate said first key and said second key.

48. The access controller of claim 45, wherein said first key is a public encryption key and said second key is a private encryption key complementary to said public encryption key.

49. The access controller of claim 45, wherein a medium for connecting said interface and said client is selected from the group consisting of an RS-232 cable, a USB cable, the Internet, the PSTN, a local area network, and a wireless network.

50. The access controller of claim 45, wherein said computer is a telecommunications switch.

51. (*cancelled*)

52. The access controller of claim 45, wherein said instructions are encrypted by said client using said first key and said verification protocol is based on a successful decryption of said instructions by said access controller using said second key.

53. (*cancelled*)

54. The access controller of claim 45, wherein said first key is obtained by said client only if a user operating said client authenticates said user's identity with said authentication server.

55. The access controller of claim 45, wherein said access controller contains a preset second key and said authentication server maintains a record of said preset second key; said authentication server operable to deliver said first key and said second key only if said access controller successfully transmits said preset second key to said authentication server and said transmitted preset second key matches said authentication server's record thereof.

56. (*withdrawn*)

57. (*withdrawn*)

58. (*withdrawn*)

59. (*withdrawn*)

60. (*withdrawn*)

61. (*withdrawn*)

62. (*withdrawn*)

63. (*withdrawn*)

64. (*withdrawn*)

65. (*withdrawn*)

66. (*withdrawn*)

67. A method of securing access between a client and a computer having an access controller intermediate said client and said computer, said method comprising:

receiving an instruction at said client destined for said computer;

generating a random number by said client;

encrypting said random number by said client using a first key;

delivering said random number, said encrypted random number and said instruction to said access controller;

decrypting said encrypted random number using a second key by said access controller, said second key complementary to said first key;

comparing said random number and said decrypted number;

passing at least a portion of said instruction to said computer if said comparison finds a match of said random number with said decrypted number; and,

discarding said at least a portion if no match is found.

68. An authentication server, comprising:

an interface for communicating with a client and an access controller via a communication medium; and

a processing unit operable to determine a first key for delivery to said client and a second key for delivery to said access controller, said first key being delivered to said client only after said second key has been successfully delivered to said access controller; such that when said access controller and said client are connected, said access controller selectively passes instructions from said client to a computer attached to said access controller if a verification protocol utilizing said keys is met.

69. The authentication server of claim 68, wherein said processing unit is operable to generate said first key and said second key.

70. (*withdrawn*)

71. (*withdrawn*)

72. (*withdrawn*)

73. (*withdrawn*)

74. (*cancelled*)

75. (*cancelled*)

76. (*cancelled*)

77. (*cancelled*)

78. (*cancelled*)

79. (*cancelled*)

80. (*cancelled*)

81. (*cancelled*)

82. (*cancelled*)

83. The method according to claim 35, wherein said first key is delivered to said client only if a user operating said client authenticates said user's identity with said server.

IX. 37 CFR §41.37 (c)(1)(ix) - Evidence Appendix

None.

X. 37 CFR §41.37 (c)(1)(x) - Related Proceedings Appendix

None.

CONCLUSION

It is respectfully submitted that claims 35-41, 44-45, 47-50, 52, 54-55, 67-69 and 83 are in condition for allowance as they currently stand. Reconsideration of the rejections and objections is requested. Allowance of claims 35-41, 44-45, 47-50, 52, 54-55, 67-69 and 83 is earnestly solicited.

Respectfully submitted,

Dated: September 24, 2010

Sanro Zlobec
Reg. No. 52,535
Agent for the Applicant

SMART & BIGGAR
1000 De La Gauchetière Street West
Suite 3300
Montreal, Quebec H3B 4W5
CANADA

Customer Number: 28291

Telephone: (514) 954-1500
Facsimile: (514) 954-1396